PCT/AU03/00860 #2

AUSTRALIA

**Patent Office
Canberra**

I, LEANNE MYNOTT, MANAGER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PS 3391 for a patent by THE THREE HAPPY GUYS PTY LTD as filed on 04 July 2002.

WITNESS my hand this
Fifteenth day of July 2003

LEANNE MYNOTT
<u>MANAGER EXAMINATION SUPPORT
AND SALES</u>

P/00/009
Regulation 3.2

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION

Invention Title: **"METHOD OF MONITORING VOLUMES OF DATA BETWEEN MULTIPLE TERMINALS AND AN EXTERNAL COMMUNICATION NETWORK"**

The invention is described in the following statement:

METHOD OF MONITORING VOLUMES OF DATA BETWEEN MULTIPLE TERMINALS AND AN EXTERNAL COMMUNICATION NETWORK

The invention relates to a method of monitoring volumes of data passing between multiple terminals and an external communication network. In particular the invention relates to a method that enables an organization to monitor and control the data usage and online time of multiple terminals. However, it is envisaged that the method has other applications.

BACKGROUND TO THE INVENTION

There are now very few businesses, organizations, undertakings or the like that do not rely on one or more computer systems of one description or another. The computer system may be, at one end of the spectrum, a single desktop personal computer/workstation/terminal used by a small business with a single employee or, at the other end of the spectrum, the computer system may comprise tens, hundreds or thousands of terminals connected to the same system via a plurality of servers on different networks connected to one or more mainframe computers.

Irrespective of the size of the computer system, to access an external communication network such as the Internet, an Internet service or access provider (ISP/IAP) is required. Commonly, the ISP/IAP provides the necessary software, username(s), password(s) and the like for a monthly fee, which may be a flat fee, such as with a broadband connection, or may be dependent on the amount of online time or data transferred.

It is desirable that individual users and/or organizations are able to monitor the amount of online time and the volume of data transmitted over the connection with the external communication network, e.g. for reconciliation and security purposes.

A known method for monitoring online time is employed by, for example, Internet cafés, which enables the café to bill customers according to their period of usage at preset rates, depending on, for example, the nature of their usage, e.g. gaming, browsing, LAN. One such product is known as Geto Manager developed by Advanced Com Tech Co. Ltd and details of this product are disclosed at www.swplaza.co.kr. In this system, the start time, account details such as pre- and post- payment details, remaining time and billing rate may be monitored by and displayed on a management terminal at, for example, the counter of the Internet café. Some of these details may also be displayed on the user's terminal. Control functions available to the management terminal include automatic locking/unlocking, rebooting and/or power switch off of individual terminals. However, this product cannot monitor the data volume being used by each terminal.

Monitoring the amount of data may be carried out on individual workstations using a conventional DU meter, which shows the amount of data being downloaded and the data download rate. Details of DU meters are described at http://www.dumeter.com. However, this facility only functions relatively accurately on an individual machine. For example, in an internal network of multiple user terminals connected to the Internet, a DU meter would register all traffic coming to the terminal on which the DU meter is installed, including traffic through the Internet gateway and crosstalk between the multiple user terminals. The DU meter is incapable of discerning the function of the data packets or their origin.

Hence, there remains a need for a system and/or method that enables monitoring of data usage and time usage of any one or multiple users over multiple terminals. It is also desirable that the system and/or method enables analysis of data and time usage of the terminals and includes security measures to permit/deny access to external communication networks.

DISCLOSURE OF THE INVENTION

According to one aspect, although it need not be the only or indeed the broadest aspect, the invention resides in a method of monitoring volumes of data passing between an external communication network and each user terminal in an internal network of user terminals via a gateway, said method including the steps of:

queuing in an access queue a request for access to the external communication network from each user terminal requesting access;

reading each request;

adding or amending at least one access rule in a firewall to permit access for each user terminal requesting access based on an authenticated IP address of each user terminal; and

monitoring simultaneously at the firewall volumes of data passing between each user terminal connected to the external communication network and the external communication network.

Optionally, a single terminal may include the gateway and the firewall. Alternatively, the firewall may be in a different terminal from the gateway.

The method may further include the step of controlling access of each user terminal to the external communication network from a management terminal of the internal network.

The method may further include the step of monitoring a period of time each user terminal has access to the external communication network.

The method may further include the step of monitoring a cost to each user of their user terminal having access to the external communication network.

Further aspects of the invention will become apparent from the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

To assist in understanding the invention and to enable a person skilled in the art to put the invention into practical effect preferred embodiments of the invention will be described by way of example only with reference to the accompanying drawings, wherein:

FIG. 1 shows a schematic representation of a computer system in which the method of the present invention may be implemented; and

FIG. 2 shows a flowchart depicting the steps involved in connecting and disconnecting a user terminal to an external communication network such as the Internet.

DETAILED DESCRIPTION OF THE INVENTION

The method of the present invention may be implemented in a system such as that shown in FIG.1, but is not limited to being implemented in such systems. FIG. 1 may represent a computer system in, for example, an Internet café, a small, medium-sized or large business or other form of organization utilizing a computer system.

The system in FIG. 1 comprises one or more user terminals 4 and one or more management terminals 2 coupled to gateway 6. The management terminal(s) 2 can also be considered as user terminals. Together, user terminal(s) 4, management terminal(s) 2 and gateway 6 may be considered as an internal network. The gateway 6 may also comprise a firewall 8 employing any known firewall technique that allows customizable rules. Alternatively, the firewall 8 may be installed in a separate terminal (not shown) coupled to the gateway 6. The internal network communicates through gateway 6 with one or more external networks 10. Such external networks 10 may be the Internet, wide area networks, or secured sections of any network based on the Internet Protocol.

The method of the present invention is described with reference to the flowchart in FIG. 2. At step 20, the levels of logging, such as gaming or browsing or other functions, are set, as well as levels of pricing, if appropriate. Logging is carried out by the firewall 8 and may be carried out on a per data quantity basis e.g. Mb, and/or a per unit time basis, e.g. per second, per minute or other time period. For example, time may be logged at a preset cost per unit time and there may also be a data download limit, which, if exceeded, may incur a further charge in addition to the time spent by the user at the terminal. It will be appreciated that there are many permutations by which logging may be carried out and that the present invention is not limited to any particular permutation.

At step 22, a user logs into a user terminal 4, such as a customer in an Internet café or an employee in a business. There may be any number of pricing levels, classes or timing categories or the like, which will depend on the particular user and the application, e.g. large organization, Internet café.

With reference to step 24 in FIG. 2, if a user does not require access to an external network 10, such as the Internet, the monitoring and control method of the present invention does not come into operation and once the user has logged in they are enabled for their own network, i.e. not an external network. However, if a user does require, for example, Internet access, a request for access containing the Internet protocol (IP) address of the user's terminal is added to an access queue in the gateway 6, as represented by step 26.

When the IP address in the access queue is read by the gateway 6, the gateway generates a rule to instruct the firewall 8 to permit access to that IP address. The firewall 8 follows the rule and permits Internet access to that IP address, as represented by step 28, providing the IP address has been authenticated via a username and password at the gateway 6 for access to an external network 10. Access to an external network is granted to the user and the terminal by amending one or more rules in a list of rules followed by the firewall. The rules enable the firewall to permit or deny network access to specific IP addresses. Rules may be added or removed. Alternatively, existing rules may be changed/updated to permit or deny network access.

When external network access is enabled for a particular terminal, specific port numbers of that terminal may be enabled/disabled to permit/forbid respectively particular activities, such as gaming and/or browsing or other activities, being performed from the terminal. The particular ports enabled/disabled may depend on the particular user and/or on the particular terminal. Enabling/disabling of the ports is controlled by the rules provided to and followed by the firewall 8. A default option may be that all ports are activated to permit all activities at a terminal.

Logging of terminal activity is then commenced by the firewall 8, as represented by step 30. The type of data that will be logged includes start time, current session time, monetary cost incurred this session, user/customer limit(s) (in terms of time, expenditure and/or data volume), account type (e.g. debit or credit) and account status. Firewall 8 records such data for each particular IP address connected to the external network 10. This data can then be requested by the gateway 6 and displayed, as described hereinafter.

Once a user has logged in and gained access to the external network 10, it is not possible for the user to revert back to a previous screen prior to log in, e.g. by clicking on the “back” button, in an attempt to circumvent the monitoring and logging of their session by the method of the present invention.

Once a user has completed their session, e.g. at the end of a working day in the case of a business employee, the user logs out of the terminal, as shown at step 32. Alternatively, the gateway and firewall may cause the user to be logged out and disconnected from the external network if, for example, the user’s preset time limit has expired. This may be set such that a user’s session is terminated automatically. Alternatively, an operator of the management terminal 2 may effect session termination by initiating a disconnection request. In this way the operator can inform the user prior to session termination to avoid a user losing any important data. A user may only terminate their own session and not the session of another user unless this is done via a management terminal 2. In this case it should be an authorized staff member e.g. in the case of an organization or internet café, who will have the required username and password to use a management terminal 2.

Once logging out has been initiated, either by the user or by the request from a management terminal 2, a request for disconnection from the external network containing the IP address for the terminal to be disconnected is added to a disconnection queue in the gateway 6, as represented by step 34.

When the IP address in the disconnection queue is read, the rule(s) that permits access for that particular IP address is/are removed/amended from/in the firewall 8 and the firewall disables access to the external network for that IP address, as represented by step 36.

Once the firewall 8 has processed a queued connection request or disconnection request, that request is cleared from the queue to prevent processing of the request being duplicated in error.

A session history is maintained by the gateway 6 based on the data logs created by the firewall 8, as represented by step 38. Each session history contains relevant information for that particular user terminal and that particular user. The relevant information may include the terminal and user ID, log on and log off times, session duration, billing rate, data volume consumption/download, data download limit(s), session cost, payment method, account status and other such information. The type of information contained in the session history may be determined by the gateway and the firewall on a per user and/or per terminal basis. This information may then be compared to billing information that is supplied by the service provider.

The activity of users can be monitored at a management terminal 2 by virtue of a monitoring and control interface in the form of, for example, a table displaying which terminals are/are not in use and the relevant data associated with that terminal usage, as described above. However, the present invention is not limited to the monitoring and control interface being accessible just on a single management terminal. The interface may be accessed on any terminal in the system that has been given access to management controls.

If, for example, there is a problem with the gateway 6 or there is power loss and external network access is lost to all terminals, the present invention enables a management terminal 2 to re-connect each terminal with the external network with which it was connected before connection was lost (providing connection to the relevant external network is possible). The firewall 8 accepts a request to restore the external network connection from a management terminal 2. The firewall restores the connections to their previous status since the IP addresses of the terminals have previously been verified by the gateway 6 and enabled by the firewall 8. Each individual user does not need to request access to the external network 10 again.

The monitoring and control interface, which is accessible on whichever terminal is operating as a management terminal, offers the operator other control features including, but not limited to, a general settings feature, back up options, accounts, access settings and display/edit of staff access codes.

The general settings feature provides control over the firewall 8 and/or the gateway 6 and enables the monitoring and control method to operate as a passive booking system. This enables time slots to be allocated to particular users and/or particular terminals. Hence, if a particular time slot or terminal has been reserved and a different user attempts to log on during the reserved slot, an alert will be activated to the user and/or the management terminal 2. The operator of the management terminal may be given the option to override the time slot and/or terminal reservation.

Varying levels of security access may be set for different staff and managers and the like according to their permissions/seniority/ security clearance etc. For example staff may have their own log in screens to enable monitoring and, to an extent, control of their own terminal usage by the method of the present invention. Staff may be permitted to enable/disable external network access, but may not be able to view accounting details, which could be reserved for managerial access.

The back up options feature may, for example, provide for one or more alternative server addresses, identifications and/or passwords in the event of failure of those normally employed.

The method of the present invention enables the data related to staff/user access described above to be monitored and external network access to be controlled remotely on a per user, per machine basis and/or on a per user over multiple machines basis. This includes not only time monitoring, but also data volume usage monitoring because the traffic for each IP address, i.e. terminal, is being logged by the firewall 8 and monitored at the gateway 6.

A system employing the method is also resistant to security breaches of the system because the method monitors all traffic through the gateway 6 and firewall 8. Any attempted unauthorized access from an external terminal will require the IP address associated with the external terminal to be identified. The firewall 8 creates logs for each terminal based on the IP address of the terminal and the user ID of that terminal. The rules of the firewall will not have been altered/added to in order to permit access/traffic flow between the external terminal and the system via the firewall 8 and the gateway 6. Therefore, the external terminal should not gain access to the internal network. Furthermore, the method restarts the firewall periodically after a short time period, e.g. 2 seconds, has elapsed. Therefore, in the event that the unauthorized external terminal disables the firewall 8, it will be restarted within a short time to once again deny access to the unauthorized external terminal. Any activity of the unauthorized external terminal will therefore be identified because their activities will be logged and the unauthorized external terminal will be identified by an alert on the management terminal(s).

The present method also allows for permitting access to authorized remote terminals that are not part of the internal network shown in FIG. 1. In this case, the gateway 6 will have authorized the IP address and user code for the remote terminal in advance of a log in request. The advance authorization may be conducted via, for example, email. This applies to both permanent and temporary external IP addresses. Their activities will also be displayed on the management terminal(s).

The method of the present invention operates on any known operating system that has HTML capability on the staff/user terminals. Where the server side needs more than HTML capabilities, it has to be configured to the appropriate operating system's gateway/firewall structures.

Throughout the specification the aim has been to describe the invention without limiting the invention to any one embodiment or specific collection of features. Persons skilled in the relevant art may realize variations from the specific embodiments that will nonetheless fall within the scope of the invention.

Dated this Fourth day of July 2002

THE THREE HAPPY GUYS PTY LTD

By their Patent Attorneys

FISHER ADAMS KELLY

14

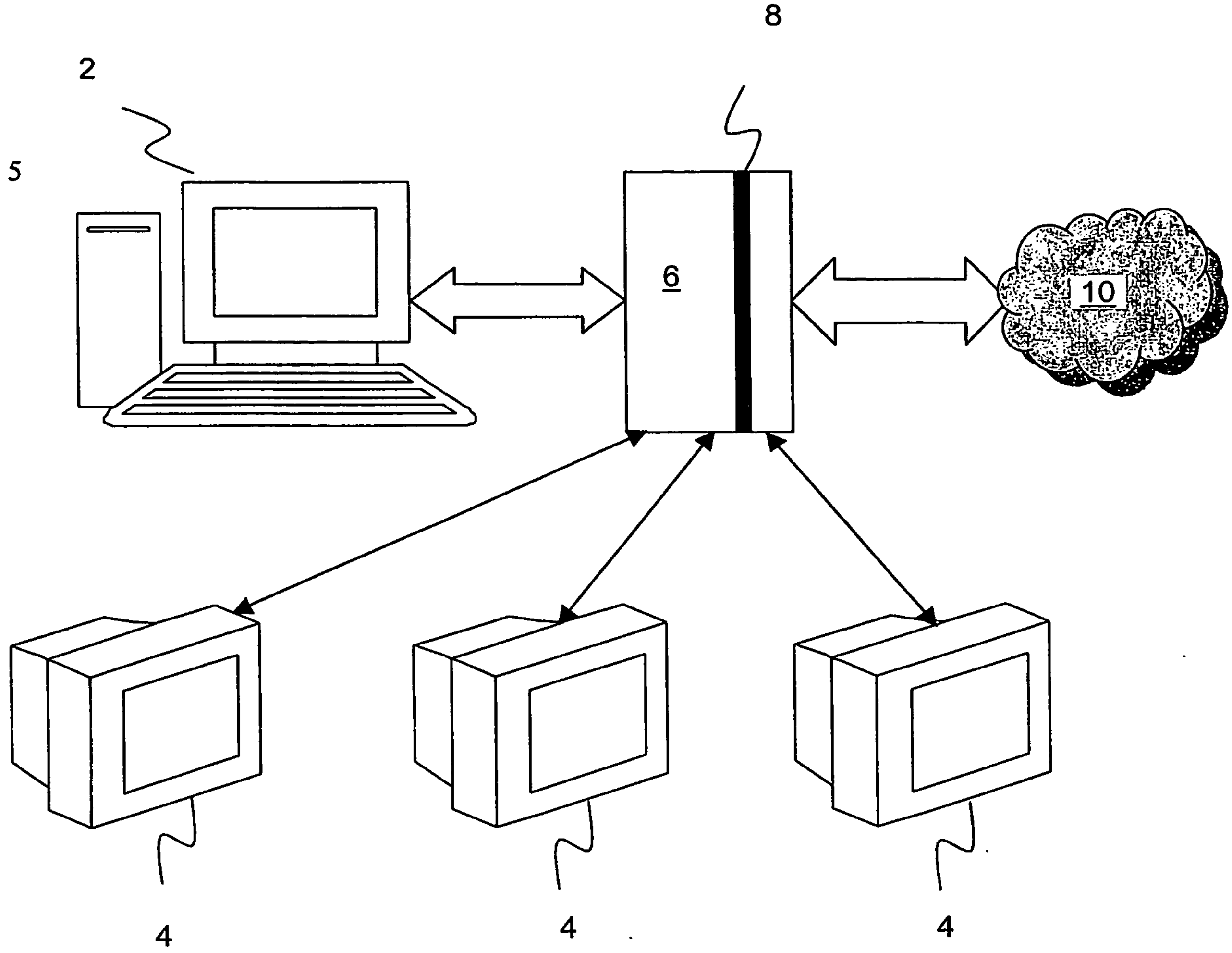

FIG. 1

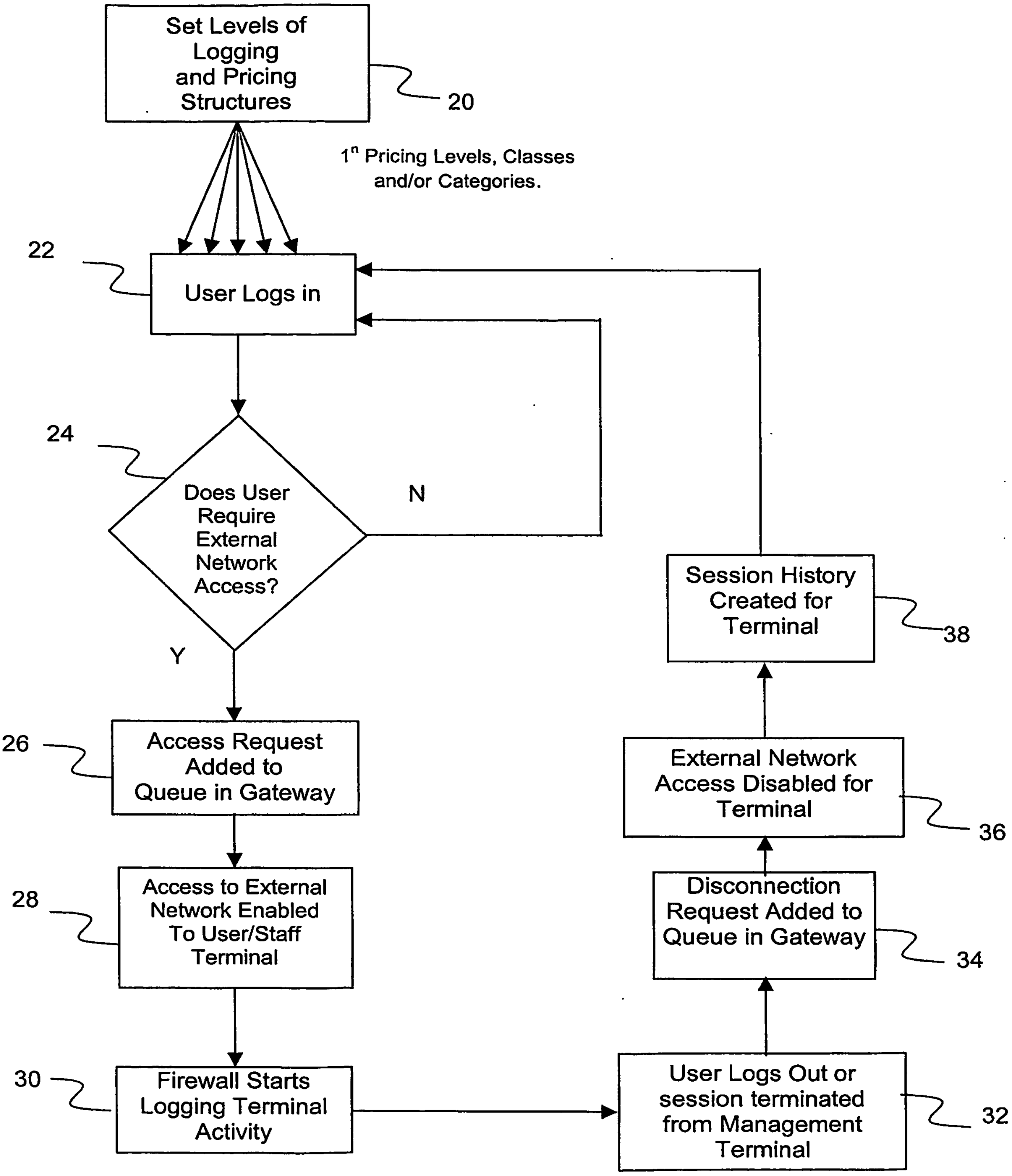
Set Levels of Logging and Pricing Structures
20
1ⁿ Pricing Levels, Classes and/or Categories.
22
User Logs in
24
Does User Require External Network Access?
N
Y
26
Access Request Added to Queue in Gateway
28
Access to External Network Enabled To User/Staff Terminal
30
Firewall Starts Logging Terminal Activity
User Logs Out or session terminated from Management Terminal
32
Disconnection Request Added to Queue in Gateway
34
External Network Access Disabled for Terminal
36
Session History Created for Terminal
38

FIG. 2